IN THE CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method for the generation of forgery-proof documents or data records, whereby key information is generated and whereby encrypted checking information is formed from the key information and from a transaction indicator,

comprising the steps of

generating ~~random~~ key information in a contact station; ~~and~~

forming encrypted checking information from the key information and from [[a]] the transaction indicator in ~~a cryptographically reliable~~ the contact station,

encrypting the key information in the ~~cryptographically reliable~~ contact station,

transmitting the encrypted checking information and the encrypted key information ~~by the cryptographically reliable contact station~~ to an intermediate station,

~~the intermediate station temporarily~~ storing the encrypted key information and the encrypted checking information in the intermediate station and subsequently transmitting ~~this~~ the encrypted key information and the encrypted checking information to a cryptographic module ~~of a document producer~~ at a different ~~point in~~ time from the transfer between the ~~cryptographically reliable~~ contact station and the intermediate station.

2. (Currently Amended) The method according to Claim 1, comprising

randomly generating the key information ~~in such a way that the key information is formed randomly~~.

3. (Previously Presented) The method according to Claim 1, comprising

configuring at least one of the encrypted key information and the encrypted checking information in such a way that it cannot be decrypted in the intermediate station.

4. (Currently Amended) The method according to Claim 1, comprising ~~the cryptographic module~~ decrypting the encrypted key information with a key contained in the cryptographic module.

5. (Currently Amended) The method according to Claim 1, comprising ~~the document producer~~ entering ~~his own~~ document data into the cryptographic module.

6. (Currently Amended) The method according to Claim 1, comprising irreversibly linking the document data ~~entered by the document producer~~ to the key information ~~by means of the cryptographic module~~.

7. (Currently Amended) The method according to Claim 6, comprising irreversibly linking the document data ~~entered by the document producer~~ and the ~~decrypted~~ key information by ~~using the key information to form~~ forming a check value from the key information ~~for the document~~.

8. (Currently Amended) The method according to Claim 6, comprising combining the document data and the key information that is irreversibly linked to the document data to form ~~forming~~ at least one of a document and a data record ~~from the result of the irreversible linking of the data entered by the document producer with the decrypted key information~~ and transmitting the document or data record to a checking station.

9. (Currently Amended) The method according to Claim 8, wherein the document or data record transmitted to the checking station ~~contains the document producer's own data,~~ is transmitted at least partially in plain text.

10. (Previously Presented) The method according to Claim 8, comprising entering the encrypted checking information into the document or data record that is transmitted to the checking station.

11. (Previously Presented) The method according to Claim 1, comprising encrypting information remaining in the cryptographic module in such a way that it can be decrypted in the cryptographic module.

12. (Currently Amended) The method according to Claim [[1]] 11, comprising supplying the cryptographic module with the information~~, also in case of a supply via communication partners that are not reliable in the cryptographic sense, by~~ from a cryptographically reliable station ~~whose information~~ that can be relied on by the checking station.

13. (Currently Amended) The method according to Claim 12, comprising ~~in order for a reliable station to provide reliable information for the cryptographic module,~~ using cryptographic encryptions that the checking station can reverse.

14. (Currently Amended) The method according to Claim [[1]] 12, comprising supplying the cryptographic module via communication partners that are cryptographically non-reliable ~~in such a way that~~ and forwarding ~~the~~ information ~~is forwarded~~ to the cryptographic module at a different point in time from the transfer of information between the contact station and the intermediate station.

15. (Currently Amended) The method according to Claim [[1]] 12, comprising supplying the cryptographic module via communication partners that are cryptographically not reliable in such a way that an exchange of information within a dialog is not necessary.

16. (Currently Amended) The method according to Claim 1, comprising cryptographically linking ~~the two types of data~~ the key information and the encrypted checking information to each other, such that said linking cannot be discovered by means of crypto-analysis.

17. (Currently Amended) The method according to Claim [[19]] 16, wherein the cryptographic linking of the ~~two types of data~~ key information and the encrypted checking information is such that non-linear fractions are added that are known only to the reliable contact station and to the checking station.

18. (Previously Presented) The method according to Claim 1, wherein the generated forgery-proof documents or data records contain monetary value information.

19. (Currently Amended) The method according to Claim 18, comprising cryptographically connecting the monetary value information to the document or data record, and forming ~~in such a way that~~ a check value ~~can be formed~~ by comparing the monetary value information to the document or data record.

20. (Previously Presented) The method according to Claim 18, wherein the monetary value information contains proof of the payment of postage amounts.

21. (Currently Amended) The method according to Claim 20, comprising linking the monetary value information ~~that proves the payment of postage amounts~~ to identification data ~~of the document producer~~.

22. (Previously Presented) The method according to Claim 20, comprising linking the monetary value information to address data.

23. (Currently Amended) A value transfer center with an interface for loading monetary values, comprising

an interface to receive encrypted information [[of]] from a cryptographically reliable contact station and to temporarily store the ~~received~~ encrypted information; ~~as well as~~

a means ~~for~~ of receiving value transfer requests [[by]] from at least one cryptographic module; and

a means of forwarding the ~~received~~ encrypted information to the cryptographic module at a different point in time from a transfer of information between the cryptographically reliable contact station and the interface.

24. (Previously Presented) The value transfer center according to Claim 23, wherein the information is encrypted in such a way that it cannot be decrypted in the value transfer center.